Int. J. Adv. Sci. Eng. Vol.6 No.2 1313-1317 (2019) **1313** *E-ISSN: 2349 5359; P-ISSN: 2454-9967*

RESEARCH ARTICLE

Design and Implementation of Finger Print Based Intelligent Automated Teller Machine

S.Sumathi, P.C Sivakumar, M. Dharmalingam
Department of Electrical and Electronics Engineering, Mahendra Engineering College,
Mallasamudram - 637 503, Namakkal District, Tamil Nadu, India.

ABSTRACT: This paper presents a novel approach to improve the service of ATM cash withdrawal in less time with high level security. The idea behind this work is to add more than one bank account in an ATM machine, so that the user need not carry more cards with them and to avoid complication of handling of passwords. In these systems, Bankers will collect the customer finger prints and mobile number while opening the accounts then customer only access ATM machine. The people recognition using biometrics can have more security compared to other traditional method.

KEYWORDS: ATM, Biometric, Fingerprint, PIN, security

https://doi.org/10.29294/IJASE.6.2.2019.1313-1317

© 2019 Mahendrapublications.com, All rights reserved

1. INTRODUCTION

An ATM is a computerized telecommunications device that enables the clients of any financial institution to perform financial transactions like deposits, transfers, balance enquiries, mini statement, and withdrawal of fast cash. The ATM machine has card reader and keys as input devices and video display, cash dispenser, receipt printer, speaker as output devices. ATM is connecting to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, freelance service suppliers owned this host processor. At present, each client has a private ATM card for each and every bank during which the client maintains their accounts. So handling the cards, passwords play a serious role here.

ATM smart machine, so that the user can select the bank an interest to hold out dealings. Biometric technology is the most widely accepted and mature biometric method and is the best to deploy and for a higher level of security. Using biometric identifiers offers several advantages over traditional and current strategies. It is simple to put in and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device. Thus, fingerprint recognition is taken into account among the smallest amount intrusive of all biometric verification techniques. Though fingerprint pictures square measure at first captured, the photographs don't seem to be keep anyplace within the system. Instead, the fingerprints square measure regenerate to templates from that the original fingerprints cannot be recreated; hence no misuse of system is possible.

The user will manage accounts in numerous banks with the assistance of this single positive identification that provides quick access and reduces the quality of managing more than one ATM card and their passwords. This also leads to lessen the transaction charges that were lived on the users/customers for transaction and decrease in the production of smart cards for each every account (1-3).

Cards are used for the cause of money transactions which play integral function in day to day life. The password and PIN number caused the leakage of information stored in ATM smartcard which lead to misuse the lost of money in bank account and private information (4). Bankers will collect the customer finger prints and mobile number while opening the accounts then customer only access ATM machine. The working of these ATM machine is when customer place finger on the finger print module when it access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller(5-6). Biometric authentication includes fingerprint, palm print, and handprint, face recognition, speech recognition, dental and eye biometrics (7). The metric used for performance of identification techniques are directly scanned fingerprints or inked impression of fingerprints (8-10) When the client enters ATM and when inserting card he should place finger on the finger print module then he get mechanically generated 4-digit code when as a message to the mobile of the licensed client through GSM electronic equipment connected to the microcontroller (11). The code received by the client ought to be entered by pressing the keys on the bit screen, when solely that he are ready for additional dealing. Biometrics can give bigger security and convenience than ancient ways for individual's recognition. Even if we

**Corresponding Author: sumathis@mahendra.info*

Received: 11.08.2019 **Accepted:** 18.10.2019 **Published on**: 30.11.2019

have a tendency to don't wish to exchange a classic technique (password or hand-held token) by a biometric one, for sure, we have a tendency to area unit potential users of those systems, which will even be mandatory for new passport models.

The security options were increased mostly for the soundness and reliableness of owner recognition. The whole system is constructed on the technology of embedded system that makes the system safe, reliable and simple to implement. Hence the vulnerabilities of the ATM fraud are going to be reduced in future. A biometric primarily based identification system instead of card based transactions. The key intention is to map multiple account using a single fingerprint. This system reduces the requirement to maintain a card for each account. This system works employing a scanner, followed by a hashing algorithm and decoding. Each group action generates a key which is verified from the database. Figure 4, shows a flow graph of such a system (12).

3. METHODOLOGY

The customer finger prints are read in R305 finger print sensor and details are stored in PIC 16F628A. The bank details of each individual customer are stored in the software of ATM machine through lab view software. The interface of Universal Asynchronous Receiver/Transmitter (UART) data in the micro controller and synchronize them in Lab View Software. When the customer enrolls thumb, they can access different bank accounts which will be displayed in the monitor of ATM machine shown in Figure 1.

An Automated Teller Machine (ATM) is an electronic device that allows a bank's customers to make cash withdrawals and check their account balances without the need or human teller. Many ATMs additionally enable individuals to deposit money or cheques, transfer cash between their bank accounts, high up their mobile phones postpaid or maybe get postage stamps. In hottest ATMs, the client identifies him or herself by inserting a plastic card with magnetic strip or plastic revolving credit with a chip that contains his other account number. The customer then verifies their identity by entering a password (i.e.) personal identification number (PIN) of four digits (6) shown in Figure 2.

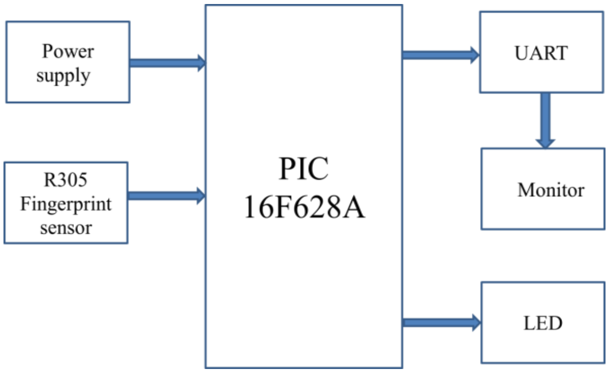


Figure1 : Block diagram: multi account handling in ATM machine

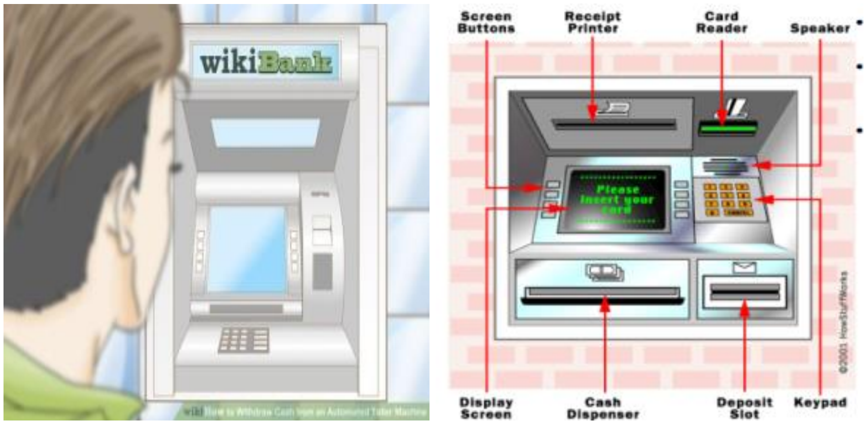


Figure 2 : Automatic Teller Machine

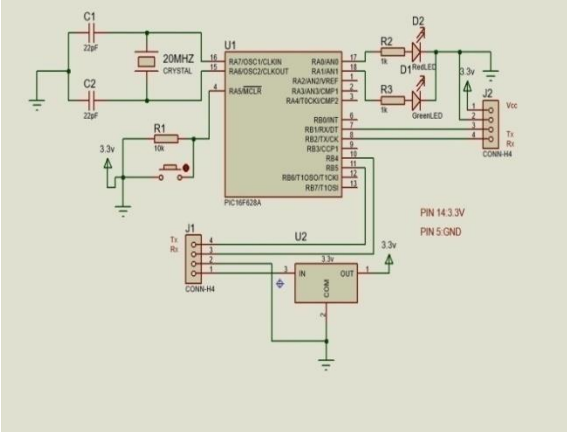


Figure 3: Multi account handling in ATM machine

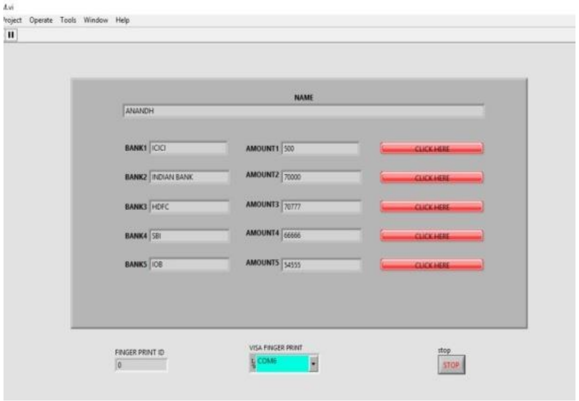
If the amount is entered incorrectly several times consecutively (usually three), most ATMs can retain the cardboard as a security precaution to forestall AN unauthorized user type discovering the PIN by guesswork and so on. Moreover there's a limitation in group action for the opposite bank customers in mistreatment the ATM of another bank crossing the limit they need to pay group action fees. By scratching the ATM card into the machine and getting into identification number, one will simply perform group action, transfer cash, etc.PIN number is a crucial aspect used to secure information of customer's account, thus should not be shared with others. In this regard, AN intuitive approach is to introduce identity verification technique in ATM systems, i.e., face recognition technique from 3 different angles using high resolution camera.

The idea behind this universal ATM machine is that the customers can use a single ATM machine to operate different bank accounts instead of having individual machine for each bank account and maintaining their pin's. The technology behind the product of the service is that adding all the user bank accounts to a universal ATM machine. In this the user should enroll their thumb in finger print sensor. After this process the ATM machine monitor display the various accounts of the customer, then it request for authentication in the server side. After the user is authenticated for individual login, the user can select the bank from which he/she is willing to perform transaction. After choosing the bank the request is shipped to the corresponding bank through a network and links it with the banks server for accessing the information of the user or customer so that the transaction is processed shown in Figure 3.

4. RESULTS AND DISCUSSION

The handling of multiple accounts in the ATM machine may help the customer to handle various accounts in a simple way and also avoids the holding of many ATM cards. The proposed method makes the banking accounts more compact and consist. Lab view software is used to design the working of ATM. The switching operation is made with the help of lab view tool. Embedded software is used to code the details of the customer. In future most of the projects used in display figure print sensor is used, which make the system more advanced.

A Queuing Message Telemetry Transport (MQTT) session is divided into four stages: connection, authentication, communication and termination. A client starts by creating a TCP/IP connection to the broker by using either a standard port or a custom port defined by the broker's operators. When creating the connection, it is significant to identify that the server strength and maintain an old session if it is provided with a reused client identity. The standard ports are 1883 for non-encrypted communication and 8883 for encrypted communication using SSL/TLS. During the SSL/TLS handshake, the client validates the server certificate to authenticate the server. While not specifically part of the MQTT specification, it has become customary for brokers to support client authentication with SS L/TLS client-side certificates in Figure 4 to Figure 6. This work mainly focused on internet of things is interrelated to the computing devices such as mechanical and digital machines people that are USED with Unique identifiers (UIDs) and the capacity to transmit data over a network not including the required human-to human or human-to-computer interaction with customer finger prints and mobile number.



NAME: ANANDH

BANK1: ICICI AMOUNT1: 500

BANK2: INDIAN BANK AMOUNT2: 70000

BANK3: HDFC AMOUNT3: 70777

BANK4: SBI AMOUNT4: 66666

BANK5: IOB AMOUNT5: 54555

FINGER PRINT ID: 0

VISA FINGER PRINT: COM6

Figure 4 : Display of IoT application

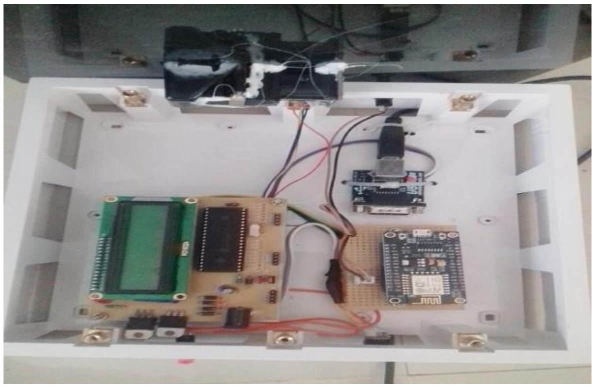
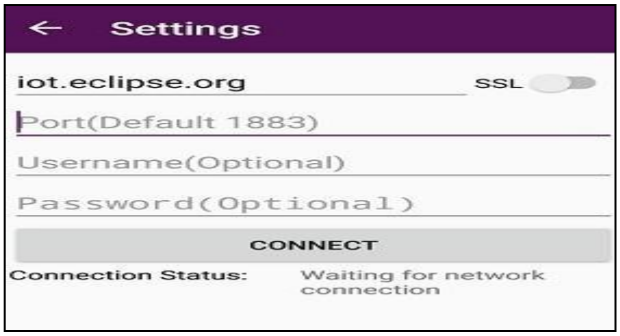


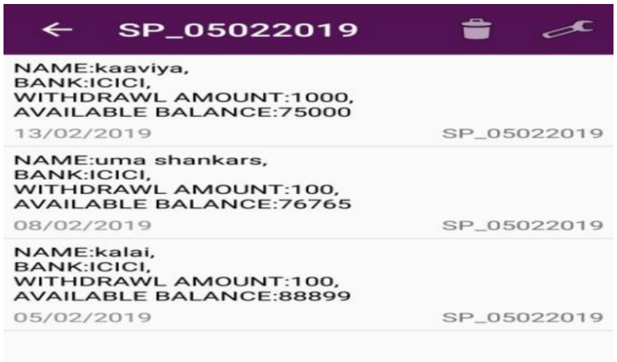
Figure 5: Hard ware of multi account handling in ATM machine



iot.eclipse.org

Connection Status: Waiting for network connection

Figure 6 (a): Display of ATM Software



NAME:kaaviya,
BANK:ICICI,
WITHDRAWL AMOUNT:1000,
AVAILABLE BALANCE:75000
13/02/2019 SP_05022019

NAME:uma shankars,
BANK:ICICI,
WITHDRAWL AMOUNT:100,
AVAILABLE BALANCE:76765
08/02/2019 SP_05022019

NAME:kalai,
BANK:ICICI,
WITHDRAWL AMOUNT:100,
AVAILABLE BALANCE:88899
05/02/2019 SP_05022019

Figure 6(b): Display of ATM Software

5. CONCLUSION

A fingerprint as a biometric measure to enhance the security features of the ATM for effective banking transaction. The developed application has been found promising on unique fingerprint authentication for multiple accounts of its sensitivity to the popularity of the shoppers finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account. An embedded fingerprint biometric authentication schemes to implement multiple accounts ATM banking for more security and easy to handle the transactions. The performance of ATM security by with fingerprint recognition and GSM MODEM took reward of the stability and reliability of fingerprint distinctiveness. Further, the system contains the method of original verifying input owner's password which is drive by the controller. The protection features were improved mainly for the stability and reliability of owner recognition. The entire system was build on the fingerprint technology which makes the system more in safe hands, consistent and simple to use. In future the unknown person entering wrong finger print to access another person’s account that person detail also indicated to the bank with the help of fingerprint.

REFERENCES

[1]. Mithun Dutta., KangkhitaKeam Psyche., ShamimaYasmin.,(2018). ATM Transaction Security Using Fingerprint Recognition. American Journal of Engineering Research , 6(8) 41-44.

[2]. SavitaChoudhary.,(2017). Design of Biometric Based Transaction System using Open Source Software Development Environment. International Conference On Advances in Computer & Communication Engineering Organized by Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India .

[3]. DhirajSunehra., (2014). Fingerprint Based Biometric ATM Authentication System, International Journal of Engineering Inventions 3(11) 22-28.

[4]. MithunDutta., Kangkhita Keam and ShamimaYasmin., (2017). ATM Transaction Security Using Fingerprint Recognition, American Journal of Engineering Research, 6(8) 41.46.

[5]. MaheshA.PatilSachinP.Wanere., (2016). ATM Transaction Using Biometric Fingerprint Technology, International Journal of Electronics, Communication & Soft Computing Science and Engineering , 2(6) 36.40.

[6]. Savita Choudhary., (2014). Design of Biometric Based Transaction System using Open Source Software Development Environment, International Conference On Advances in Computer & Communication Engineering Organized by Department of CSE & ISE, Vemana Institute of Technology, Bengaluru, India .

[7]. Dhiraj Sunehra.,(2014). Fingerprint Based Biometric ATM Authentication System, International Journal of Engineering Inventions, 3(11) 22.28.

[8]. G.SambasivaRao., C. NagaRaju,, L. S. S. Reddy and E. V. Prasad .,(2015). A Novel Fingerprints Identification System Based on the Edge Detection, International Journal of Computer Science and Network Security, 8(3) 394.397.

[9]. Robert Hastings., (2007). Ridge Enhancement in Fingerprint Images Using Oriented Diffusion, IEEE Computer Society on Digital Image Computing Techniques and Applications, 2(2) 245.252.

[10]. JinweiGu, Jie Zhou., and ChunyuYang., (2006). Fingerprint Recognition by Combining Global Structure and Local Cues, IEEE Transactions on Image Processing, 15(7) 1952.1964.

[11]. BhawnaNegi.,Varun Sharma.,(2011), Fingerprint Recognition System, International Journal of Electronics and Computer Science Engineering 872 .

[12]. Robert Hastings (2007). Ridge Enhancement in Fingerprint Images Using Oriented Diffusion, IEEE Computer Society on Digital Image Computing Techniques and Applications, pp 245-252.

[13]. Jinwei Gu., Jie Zhou., and Chunyu Yang (2006). Fingerprint Recognition by Combining Global Structure and Local Cues, IEEE Transactions on Image Processing,. 15(7) 1952 – 1964.

All © 2018 are reserved by International Journal of Advanced Science and Engineering. This Journal is licensed under a Creative Commons Attribution-Non Commercial-ShareAlike 3.0 Unported License.